Proceedings of the 4th International Conference on Signal Processing and Machine Learning
DOI: 10.54254/2755-2721/47/20241133

A comparative analysis of blockchain attack classifications

Zichao Wang

Department of Chemistry, University of Manchester, Manchester, M13 9PL, United Kingdom

zichao.wang-3@student.manchester.ac.uk

Abstract. As blockchain technology has evolved, it has introduced an array of functionalities and mechanisms. However, this advancement has also attracted a growing number of threats specifically targeting blockchains, heightening concerns regarding blockchain security. Although several researchers have attempted to categorize blockchain attacks in their respective studies, there remains a significant disparity among these taxonomies. This paper delves into three distinct classification methodologies, comparing their respective strengths and weaknesses. Additionally, it offers insights into the essential attributes that a comprehensive and effective taxonomy should possess. By breaking down each classification method, the paper provides a clearer understanding of how various researchers approach the challenge of categorizing blockchain threats. This includes looking at the criteria each method uses, such as the level of technical sophistication required for each attack, the potential damage inflicted, or the underlying motivations of the attackers. Furthermore, the paper emphasizes the importance of a universally accepted taxonomy, as this would not only facilitate more effective communication among researchers but also help in devising better defense mechanisms. In conclusion, by analyzing and comparing these classification methodologies, the study hopes to pave the way for a more unified and comprehensive approach to understanding blockchain security threats in the future.

Keywords: Blockchain, Blockchain Attack, Classification, Taxonomy.

1. Introduction

The categorization of blockchain attacks remains pivotal in both understanding and mitigating threats that jeopardize the robustness and transparency of blockchain networks. While blockchain technology is lauded for its decentralization and heightened security, it isn't immune to sophisticated adversarial exploits. Ensuring the resilience of these networks demands a thorough understanding of the multifaceted attacks targeting its distinct layers and components, from meddling with transactional data and smart contracts to disrupting consensus mechanisms or infringing on user privacy. In this analysis, we venture into the variegated threat landscape, dissecting attack methodologies and the subsequent defensive strategies implemented to shield the blockchain's intricate ecosystem. Grasping these classifications is quintessential for blockchain's ongoing refinement and fortified security. To provide a holistic perspective, three prominent classification paradigms have been identified, each of which will be juxtaposed to discern their inherent features and the nuances that differentiate them.

DOI: 10.54254/2755-2721/47/20241133

2. Analysis of Existing Surveys

2.1. Classification by Layer of Attack Occurrence

Within the multifaceted architecture of blockchain technology, six distinct layers emerge: the data layer, network layer, consensus layer, incentive layer, contract layer, and application layer. A comprehensive study by Hameed et al. delves into classifying applications within the realm of 'blockchain 4.0'. This examination not only stratifies attacks by their pertinent blockchain layers but also introduces their countermeasures [1]. Key facets, such as the nature of the attack, objectives of the attacker, ensuing security breaches, exploited vulnerabilities, and targeted applications, are comprehensively detailed in the study. The data layer showcases seven prominent attacks: Malleability attack [2], Time Hijacking, Quantum, Replay attack [3], Modification, Fault injection, and the Upgraded attack. Delving into the network layer, ten distinct threats surface, including the 51% attack [4], DDoS [5], Eclipse attack [6], Sybil attack [7], BGP Hijacking [8], Phishing, Liveness [9], Routing [10], Man-in-the-middle (MITM), and Blockchain ingestion. The consensus layer, though more limited, cites three main threats: Double spending [11, 12], Stake bleeding, and Cryptojacking. The incentive layer brings forth threats such as Selfish mining [13], Bribery, Refund, Block withholding, and Balance attacks. Contract layer breaches span eight types, featuring Integer overflow, Re-Entrancy, Short address, Criminal smart contract, Transaction ordering dependency [14], Timestamp dependency, Gas cost, and Mishandling exceptions. Lastly, the application layer identifies ten attacks, including Location cheating, Ballot stuffing, Badmouthing, Guess, Chosen ciphertext [15], Impersonation, Linking [16], Collusion, Private key compromise [17], and Money laundering [18, 19].

While discerning the nature, objectives, and other facets of these attacks, it becomes evident that there's no singular connecting thread. Each attack emerges with its unique characteristics. However, various countermeasures can be employed across different threats. Notably, digital signatures, consensus algorithms, and cryptographic measures appear recurrently as solutions. A consistent observation is that both digital signatures and cryptographic techniques tend to be deployed against attacks capitalizing on breaches of integrity.

2.2. Classification Based on Attack Models Affecting Blockchain Security Modules

Table 1. Attack models and attacks [20].

Classification	Attacks
Hash based attack	51% attack, Collusion attack
Centralization attack	Selfish mining, Ballot stuffing attack
Traffic attack	DoS, DDoS attack, Message spoofing attack
Network level attack	Sybil attack, Eclipse attack
Injection attack	Code injection, SQL injection, Fault injection
Integrity attack	Tampering attack, Malware (Ransomware attack, Cryptojacking attack)
Private key leakage attack	Man in middle attack, Key attack, Replay attack

The hash based attack only happened when attacker have over 51% hash value or mining power. The centralization attack would break the decentralization and make things look like centralization. The selfish mining attack is not obviously to conclude into the centralization attack, if keeping the block without sharing with others is a kind of behavior that break the decentralization, the stubborn would also be centralization attack in this taxonomy. Traffic attack would cause denial of service because of huge amount of information are filled into the network. Network level attack in this survey was not describing the network layer of blockchain, the illegal usage of accounts and authorities or the illegal occupation of hardware and software to threaten network. So some network layer attack is not include in this network level attack just like the 51% attack [21]. The injection attack described the vicious inputs into the program by unauthorized person. Integrity attack aimed to change the data, but due to the unique

DOI: 10.54254/2755-2721/47/20241133

mechanism of blockchain, change of previous data cannot be realized. The Malware attack was classified to the integrity attack, this attack is a common attack that not only occurred in blockchain. As shown in Table 1.

Table 2. Classification method and attack characters [22].

Layer	Reasons of classification	classification	Current attacking method	Attacking characteristic
Data layer	Classify by the attacker's objective	Steal the identity information of nodes	Use of deanonymization technology	According to the relevance of nodes
		Steal privacy data on chains	Use of mechanism of privacy data on chain	Attackers can get the privacy data out of authority
		Tamper the data on chain	Use of chameleon hash function	New block formed from attacker need to be accepted by majority of nodes
Network layer, Consensus layer, Incentive layer	Classify by the attacker's behavior	Publish block selectively in suitable time	Selfish mining attack, stubborn mining attack and optimized selfish mining attack	Specific state machine is needed Make forks in blockchain It might fail
		Abandon the block	Block withholding attack, block withholding with forking attack	Attack after join the mining pool Always success
		Deploy fake nodes	Sybil attack, Eclipse attack, Routing attack	Split blockchain network
		Make forks directly	51% attack, Bribery attack	Attacker have superiority on hashrate
	Classify by the attacker's objective	Get block award	Selfish mining attack, Stubborn mining attack, Optimized selfish mining attack, Block withholding attack, Block withholding with forking attack, ect.	Attackers' relative benefit increase in short term. Attackers' absolute benefit decrease in short term. Decreasing the effective computing power.
	classify by the victim	For double spending	51% attack, Bribery attack, Eclipse attack, etc.	Can realize double-spending in various way.
		Victim is all nodes on blockchain	51% attack, Bribery attack, selfish mining attack, Block withholding with forking attack, etc.	Attackers affected by the Network layer and Consensus layer parameter
		Victim is a part of nodes on blockchain	Block withholding attack, Sybil attack, Eclipse attack, Routing attack, etc.	Attackers not affected by the Network layer and Consensus layer parameter
Contract layer	The type of bug that attacker use	Only use contract bug	The DAO, etc.	No need for attacker mining, High frequency
		Use contract layer bug and other layer's bug	Attack to Fomo3D game and attack to GovernMental smart contract, etc.	Attacker need to mine blocks, Low frequency
Application layer	Factor that leads attacks	Leak or crack of private key	Dictionary attack, etc.	No obvious feature
		Bug from third party organizations	Use the bug in Digital cryptocurrency bourse	No obvious feature

The private key leakage attack was that the attacker can copy the keys when the same nonces or keys were used more than once [21]. This survey had given the solution to each attack and all of them were independent. The attacks based on the applications of blockchain were not mentioned widely in this taxonomy and the attacks based on smart contract were not discussed. As shown in Table 2.

DOI: 10.54254/2755-2721/47/20241133

2.3. Classification Considering Over-Layer Attacks

Expanding upon the concept of blockchain layers, Liu, H et al. introduced an enhanced taxonomy that presents a more functional classification. This survey offers a nuanced and comprehensive categorization, with particular emphasis on areas where over-layer attacks are most prevalent: the network, consensus, and incentive layers. Consequently, these three layers were amalgamated for a more holistic examination.

In the data layer, the taxonomy focuses on three distinct objectives of the attackers. Meanwhile, within the combined realm of the network, consensus, and incentive layers, the classification delves into four specific behaviors exhibited by attackers, two main objectives they aim to achieve, and two categories of victims they target. The contract layer's classification identifies two prevalent types of bugs responsible for the majority of attacks in this domain. For the application layer, two primary factors precipitating attacks are outlined. Table 3 presents a detailed overview of these classification methods, along with potential mitigation strategies for each type of attack. This refined taxonomy not only facilitates easier prediction and prevention of emerging threats but also ensures that the majority of attacks can be captured under this framework. The only exception noted is malware-based attacks, which stand outside this classification's purview.

Table 3. Countermeasures [23].

Reasons of classification	Classification	Countermeasure
Classify by the attacker's objective	Steal the identity information of nodes	Zero-Knowledge Proof, Ring Signature, Coin Mixing Technology
	Steal privacy data on chains	Control the Permissions of nodes, or coding a security smart contract.
	Tamper the data on chain	check the block height then compare with block height in the longest chain
Classify by the attacker's behavior	Publish block selectively in suitable time	Analyzing forking rate
	Abandon the block	Improving distribution mechanism in mining pool
	Deploy fake nodes	Deploy reliable relay node and introduce white list mechanism
Classify by the attacker's objective	Make forks directly	Stop mining pool getting too much computing power
	Get block award	Monitor the effective computing power in blockchain
	For double spending	Confirm the transaction after N blocks
classify by the victim	Victim is all nodes on blockchain	Adopt suitable parameter in Network layer and Consensus layer
	Victim is a part of nodes on blockchain	Enhancing the connectivity between nodes, refining the information transmission mechanisms among nodes, and optimizing the distribution of all nodes' positions
The type of bug that attacker use	Only use contract bug	Preventing attacks through the formal verification of smart contracts.
		Use of deanonymization tool to detect attack
	Use contract layer bug and other layer's bug	Preventing attacks through the formal verification of smart contracts.
		Use of deanonymization tool to detect attack
Factor that leads attacks	Leak or crack of private key	Preventing attacks through key escrow and adopting threshold signature technology.
	Bug from third party organizations	Enhancing application-layer software security.

DOI: 10.54254/2755-2721/47/20241133

3. Comparison of Existing Classifications

Hameed et al classified blockchain attack by blockchain layers, and the taxonomy invented by Liu [21], H et alwas based on blockchain layers. The advantage by doing this is that the classification is comprehensive enough to contain all of the blockchain attacks. As the classification by layers was over-broadly and other properties like attack nature listed in table 2 were in low correlation, it was hard to found new attacks in a short term.

Classification based on attack models affecting blockchain security moduleshas given the detailed definition of each classified attack (hash based attack, centralization attack, etc.), which was not too broad and made sure each specific attack (selfish mining attack, eclipse attack, etc.) in one class have common point or strong correlation. This made it easier to find new attacks. For example, it is more likely to find new attacks with similar character that they are all hash-based attack than finding new attacks that they are in the same layer. However this taxonomy was not friendly to forecast the countermeasures, the survey gave each attack unique method to solve without consider the correlation of countermeasures. Moreover, this taxonomy was the least comprehensive compared with other two taxonomies, the most intuitive example was that the smart contract layer attack was not mentioned in this classification.

Classification considering over-layer attacks gave the same countermeasures to each objectives, behaviors, etc. This would make it more efficient when finding the countermeasure of new attacks.

4. Proposed Classification Method and Discussion

By comparing three taxonomies, the classification considering over-layer attacks would be the best to conclude all blockchain attacks, only malware attack was not in this range. Not only the over-layer attacks were considered, the categories were classified in a strong relevance. This taxonomy better described common characteristics of attacks that belongs to the same category of attack, the process to classify new attacks would be easier and more helpful on forecast the new attacks and the countermeasures of new attacks. The future challenge might be the over-layer attacks which contain data layer attack and application layer, this kind of over-layer attack did not discuss in this taxonomy because of the lack of examples. Also, the taxonomy with higher correlation between attacks would be a direction of future work.

5. Conclusion

Blockchain attacks vary widely, yet discernible patterns and correlations emerge upon closer inspection. Studying these attacks in isolation, without seeking their interrelatedness, may impede the understanding and mitigation of newer threats. This paper presents three distinct taxonomies to classify these threats. The initial taxonomy delineates attacks based on the blockchain layers they target, namely: data, network, consensus, incentive, contract, and application layers. A more intricate classification follows, which categorizes attacks by the specific security modules they compromise within the blockchain. This includes hash-based attacks, centralization threats, traffic disruptions, network level offenses, injection schemes, integrity compromises, and private key leakages. The third and final taxonomy shifts its focus to over-layer attacks, emphasizing the intrinsic relationships between different threats. Here, data layer attacks are categorized by attacker objectives. The network, consensus, and incentive layers are differentiated by attacker behaviors, their objectives, and victim types. The contract layer classifies attacks based on specific bug types, while the application layer's threats are sorted by the underlying factors prompting the attacks. By pinpointing the critical aspects of these classification methodologies, this paper offers fresh perspectives on devising newer, more encompassing taxonomies. Such comprehensive approaches can play an instrumental role in enhancing the broader understanding of blockchain threats and their mitigation.

References

[1] Hameed, K., Barika, M., Garg, S., Amin, M. B., & Kang, B. (2022). A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives,

DOI: 10.54254/2755-2721/47/20241133

requirements, attacks, countermeasures, and open issues. Journal of Industrial Information Integration, 26, 100312.
[2] Dasgupta, D., Shrein, J. M., & Gupta, K. D. (2019). A survey of blockchain from security perspective. Journal of Banking and Financial Technology, 3, 1-17.
[3] Hajdarbegovic, N. (2014). Bitcoin miners ditch ghash. io pool over fears of 51% attack. Coindesk, January, 9.
[4] Yang, Z., Yang, K., Lei, L., Zheng, K., & Leung, V. C. (2018). Blockchain-based decentralized trust management in vehicular networks. IEEE internet of things journal, 6(2), 1495-1505.
[5] Yves-Christian, A. E., Hammi, B., Serhrouchni, A., & Labiod, H. (2018, October). Total eclipse: How to completely isolate a bitcoin peer. In 2018 Third International Conference on Security of Smart Cities, Industrial Control System and Communications (SSIC) (pp. 1-7). IEEE.
[6] Hajdarbegovic, N. (2014). Bitcoin miners ditch ghash. io pool over fears of 51% attack. Coindesk, January, 9.
[7] Zhang, Z., Zhang, Y., Hu, Y. C., & Mao, Z. M. (2007, December). Practical defenses against BGP prefix hijacking. In Proceedings of the 2007 ACM CoNEXT conference (pp. 1-12).
[8] Kiayias, A., & Panagiotakos, G. (2019). On trees, chains and fast transactions in the blockchain. In Progress in Cryptology–LATINCRYPT 2017: 5th International Conference on Cryptology and Information Security in Latin America, Havana, Cuba, September 20–22, 2017, Revised Selected Papers 5 (pp. 327-351). Springer International Publishing.
[9] Apostolaki, M., Zohar, A., & Vanbever, L. (2017, May). Hijacking bitcoin: Routing attacks on cryptocurrencies. In 2017 IEEE symposium on security and privacy (SP) (pp. 375-392). IEEE.
[10] Khalilov, M. C. K., & Levi, A. (2018). A survey on anonymity and privacy in bitcoin-like digital cash systems. IEEE Communications Surveys & Tutorials, 20(3), 2543-2585.
[11] Karame, G. O., Androulaki, E., & Capkun, S. (2012, October). Double-spending fast payments in bitcoin. In Proceedings of the 2012 ACM conference on Computer and communications security (pp. 906-917).
[12] Eyal, I., & Sirer, E. G. (2018). Majority is not enough: Bitcoin mining is vulnerable. Communications of the ACM, 61(7), 95-102.
[13] Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2020). A survey on the security of blockchain systems. Future generation computer systems, 107, 841-853.
[14] Biryukov, A. (2005). Chosen ciphertext attack.
[15] Hassan, M. U., Rehmani, M. H., & Chen, J. (2019). Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions. Future Generation Computer Systems, 97, 512-529.
[16] Mayer, H. (2016). ECDSA security in bitcoin and ethereum: a research survey. CoinFaabrik, June, 28(126), 50.
[17] Willson, C., & Taaki, A. (2017). Dark wallet.
[18] Fletcher, E., Larkin, C., & Corbet, S. (2021). Countering money laundering and terrorist financing: A case for bitcoin regulation. Research in International Business and Finance, 56, 101387.
[19] Anita, N., & Vijayalakshmi, M. (2019, July). Blockchain security attack: A brief survey. In 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
[20] Brengel, M., & Rossow, C. (2018). Identifying key leakage of bitcoin users. In Research in Attacks, Intrusions, and Defenses: 21st International Symposium, RAID 2018, Heraklion, Crete, Greece, September 10-12, 2018, Proceedings 21 (pp. 623-643). Springer International Publishing.
[21] Liu, H. Q., Ruan, N., & Zhang, L. (2021). A survey on attacking strategies in blockchain. Chin J Comput, 44(04), 786-805.
[22] Khalilov, M. C. K., & Levi, A. (2018). A survey on anonymity and privacy in bitcoin-like digital cash systems. IEEE Communications Surveys & Tutorials, 20(3), 2543-2585.

DOI: 10.54254/2755-2721/47/20241133

[23] Hameed, K., Barika, M., Garg, S., Amin, M. B., & Kang, B. (2022). A taxonomy study on securing Blockchain-based Industrial applications: An overview, application perspectives, requirements, attacks, countermeasures, and open issues. Journal of Industrial Information Integration, 26, 100312.